U.S. DEPARTMENT OF AGRICULTURE
WASHINGTON, D.C. 20250

DEPARTMENTAL REGULATION	Number: DR 3545-001
SUBJECT: Information Security Awareness and Training Policy	DATE: October 22, 2013
	OPI: Office of the Chief Information Officer

1. PURPOSE

a. This Departmental Regulation (DR) establishes the policy of the United States Department of Agriculture (USDA) for meeting the laws, regulations, and standards of a comprehensive information security awareness and training program.

b. This DR addresses guidance issued by the Office of Management and Budget (OMB), the National Institute of Standards and Technology (NIST), and the *Federal Information Security Management Act (FISMA) of 2002* requiring Federal agencies to design, develop, document, and implement an agency-wide information security awareness training program.

c. It is the policy of USDA to comply with Federal requirements to establish, implement, and support an Information Security Awareness Training program. The Department confirms the commitment of its management to comply with the authorities mandating and governing Security Awareness Training.

2. SCOPE

This policy applies to all USDA agencies and staff offices, employees, contractors, partners, and volunteers working for or on behalf of the USDA that require access to sensitive USDA information, information systems, or are otherwise directed by Federal guidance to comply with this training requirement.

3. SPECIAL INSTRUCTIONS/CANCELLATIONS

a. This regulation supersedes Departmental Manual (DM) 3545-001, Computer Security and Training, dated February 17, 2005, in its entirety.

b. This policy only addresses the awareness and training levels of the Information Technology (IT) Security Learning Continuum advocated by NIST.

4. BACKGROUND

a. OMB Circular A-130, *Management of Federal Information Resources*, establishes policy for the management of Federal information resources. Appendix III of OMB Circular A-130, *Security of Federal Automated Information Resources*, requires that prior to being granted access to IT applications and systems, all individuals must receive specialized training on their IT security responsibilities and established system rules.

b. FISMA mandates general training of employees, contractors, partners, and volunteers to ensure that they are aware of their information security responsibilities, the specialized role-based training of agency employees, contractors, partners, and volunteers with significant security responsibilities, and the reporting of agency statistics on security awareness and training efforts.

c. The Department has established an IT security awareness and training program for use throughout USDA. This DR defines the policy and strategy for IT security awareness and training within the Department.

5. POLICY

a. Information Security Awareness and Training

All USDA employees, contractors, partners, and volunteers shall be regularly and periodically exposed to information security awareness information (e.g., staff meetings, posters, awareness tools/ periodic e-mail, warning messages, tips of the day upon accessing an information system, computer/information security day events).

b. Annual Computer Based Training

(1) The Information Security Awareness Training course is a mandatory annual course for all USDA employees, contractors, partners, and volunteers.

(2) Information Security Awareness training shall provide the information security basics and literacy as described in NIST Special Publication (SP) 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003. The basics and literacy knowledge also serves as the foundation upon which role-based training is built for those with significant responsibility for information security.

(3) New USDA employees, contractors, partners, and volunteers shall complete Information Security Awareness training prior to gaining access to information systems.

(4) Federal employees, contractors, partners, and volunteers transferring from another Information Systems Security Line of Business (ISSLoB) security awareness training agency to USDA may, with verification of completion, count the information awareness and training provided by the departing agency as meeting the requirement during the fiscal year in which the training occurs. Transferred training cannot cross over into another fiscal year.

c. Role-Based Information Security Training

(1) All USDA employees, contractors, partners, and volunteers who have been identified by their agency or staff office as having significant responsibility for information security (such as those who manage, administer, operate, and design IT systems, and other senior management roles such as authorizing officials, chief information officers and information security program managers) shall receive formal role-based information security training (also known as specialized training). The amount and frequency of training depends on the gap between an individual's existing and needed skills, and changes in technology and the operating environment which the individual must adapt.

(2) Role-based Information Security Awareness training shall provide the information security basics and literacy as described in NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April 1998.

(3) All USDA employees, contractors, partners, and volunteers with significant security responsibilities shall receive role-based security-related training commensurate with their positions and duties and must be completed before access to IT system is provided.

(4) Role based Information Security Awareness Training course is a mandatory annual course for all USDA employees, contractors, partners, and volunteers with advanced IT responsibilities.

d. Training Metrics

(1) A system of record shall be maintained for all USDA IT security awareness and training curriculum, in the USDA training system of record.

(2) Identification, monitoring, tracking and reporting shall be accomplished within the Department's official system of record for security awareness training.

6. ROLES AND RESPONSIBILITIES

a. The USDA Chief Information Officer (CIO) shall:

(1) Ensure compliance with the requirements imposed under this DR, including training and oversight of personnel with significant responsibilities for information security.

(2) Establish the overall strategy for the Department's IT security awareness and training program.

(3) Ensure the USDA-wide information security program includes security awareness and training with adequate depth and scope to provide employees, contractors, partners, and volunteers with the information needed to protect the Department's systems, applications, and IT assets.

(4) Ensure that the Secretary of Agriculture, senior executives and managers, system and data owners, and others understand the concepts and strategy of the security awareness and training program, and are informed of the progress of the program's implementation.

(5) Ensure security awareness training is adequately funded through CIOs budget.

(6) Hold agency and staff office CIOs responsible for ensuring the training completion of their personnel designated as having significant security responsibilities.

(7) Direct the development of a program to ensure all personnel with access to sensitive information and/or equipment are sufficiently trained in their security responsibilities.

(8) Ensures that the Department's system of record for delivery, tracking and reporting security awareness training is in place.

b. The USDA Chief Information Security Officer (CISO) shall:

(1) Establish and implement an Information Security Training program and process as part of the USDA IT Security Program.

(2) Provide oversight of the USDA security training program.

(3) Ensure USDA implements, manages, and monitors the USDA security training program for compliance with applicable Federal laws, Executive Orders, directives, policies, and regulations. The USDA CISO reports directly to the USDA CIO and is the principal advisor for training policy.

(4) Develop the department's information security awareness training course(s).

(5) Approve the content of any information security awareness training courses developed by the agencies.

(6) Review the department's information security and awareness training policy annually.

c. The Associate CIO for Agriculture Security Operations Center (ACIO-ASOC) shall:

(1) Ensure guidance, tools, and strategies to assist USDA agencies in complying with the requirements of this policy are in place and documented.

(2) Ensure the Information Security Training program provides administration, technical support, and training in the use of the Department's official system of record.

(3) Ensure agency management of activities related to Information Security Training is in place and functioning in accordance with Federal guidelines.

d. Agency and Staff Office CIOs shall:

(1) Develop, conduct, and implement their own agency-specific IT security awareness and training program based on the Department's program, guidance and utilizing the Department security awareness training courses and security awareness training system of record. Additionally, each USDA agency and staff is responsible for developing agency-specific procedures which ensure compliance with this DR.

(2) Although the agency must utilize the department's basic security awareness and role based training courses, additional training material for role based training should be considered based on the specific roles, requirements and environment of the agency.

(3) Utilize the Department's security awareness training system of record to monitor, track, and report on all IT security awareness and IT role-based security training.

(4) Develop, organize, implement, and maintain an agency/staff office level IT security awareness and training program in compliance with FISMA to ensure the security of agency information and IT assets. Agency training may enhance, but cannot replace or conflict with the Department's mandatory information security awareness and training requirements as addressed in this policy.

(5) Develop and document a process to ensure their agency's employees, contractors, partners, and volunteers receive security awareness training and any necessary specialized training required by this directive and NIST training guidance.

(6) Ensure all agency employees, contractors, partners, and volunteers have accounts in the official USDA training repository (currently AgLearn) to enable electronic tracking of statistical training performance measures as required by FISMA.

(7) Ensure all users are appropriately trained to fulfill their security responsibilities based on their roles, responsibilities, duties, and need-to-know before allowing them access to any USDA information or information system.

(8) Ensure computer security training requirements are explicitly addressed in all new IT system acquisitions, specifications, statements of work, grants, and cooperative agreements. These requirements should reflect the appropriate level of awareness and training based on job functions and access required.

(9) Designate federal employee(s) to serve as administrator(s) of the agency's data in the Department's system of record for security awareness training.

e. The Agency and Staff Office Information Systems Security Program Managers (ISSPMs) shall:

(1) Implement and document the processes necessary to ensure all agency employees, contractors, partners, and volunteers receive the security awareness and training and any necessary specialized role-based training for those with significant IT security responsibilities as identified in NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance Based Model*, April 1998, and this policy.

(2) Ensure that all agency/staff office employees, contractors, partners, and volunteers have completed the mandatory annual Information Security Awareness Training course presented in the Department's electronic training system.

(3) Ensure that agency/staff office employee security awareness and role-based training completions are recorded appropriately in the Department's system of record; and

(4) Coordinate with agency/staff office personnel responsible for preparing procurement requests, Acquisition Approval Requests (AARs), grants and service agreements to

ensure that these and other procurement documents contain the USDA training requirement language.

f. The Agency Administrators for the Department's System of Record shall:

(1) Ensure the number of employees, contractors, partners, and volunteers are updated annually in the Department's system of record.

(2) Ensure that the data associated with the training of those users is accurate.

(3) Maintain supporting documentation of the data recorded in the training repository.

(4) Ensure employees, contractors, partners, and volunteers who complete security training using an alternative method (i.e., paper-based training) have their course completion information documented in the Department's system of record.

g. USDA managers and supervisors at all levels shall:

(1) Complete annual IT security awareness training as required by this DR.

(2) Ensure their employees, contractors, partners, and volunteers complete annual IT security awareness training as required by this DR.

(3) Report any known violation of this IT security policy to their agency ISSPM.

(4) Be fully informed of the USDA information security directives.

(5) Provide to employees DR4070-735-001, *Employees Responsibilities and Conduct* and DR 3300-001, *Telecommunications and Internet Services and Use*.

h. USDA employees, contractors, partners, and volunteers shall:

(1) Complete annual IT security awareness training as required by this DR and identified by supervisors or agency project managers.

(2) Report any known violation of this IT security policy to their agency ISSPM or immediate supervisor.

(3) Complete role based training before making changes to any USDA software, hardware, and system or network device.

(4) Review with supervisor DR4070-735-001, *Employees Responsibilities and Conduct* and DR 3300-001, *Telecommunications and Internet Services and Use*.

7. PENALTIES AND DISCIPLINARY ACTIONS FOR NON-COMPLIANCE

DR4070-735-001, *Employee Responsibilities and Conduct*, Section 16, sets forth the USDA's policies, procedures, and standards on employee responsibilities and conduct relative to the use of Computers and Telecommunications Equipment, with further delineation provided in DR 3300-001, *Telecommunications and Internet Services and Use*, Section3. In addition, DR 4070-735-001, Section 21, Disciplinary or Adverse Action states:

a. *A violation of any of the responsibilities and conduct standards contained in this directive may be cause for disciplinary or adverse action.*

b. *Disciplinary or adverse action shall be effected in accordance with applicable law and regulations*.

Such disciplinary or adverse action shall be effected in accordance with applicable law and regulations such as the Code of Ethics for Government Employees, Office of Personnel Management regulations, Office of Management and Budget (OMB) regulations, and Standards of Conduct for Federal Employees. Therefore, these rules carry the same responsibility for compliance as the official documents cited above.

8. POLICY EXCEPTIONS

a. All USDA agencies and staff offices are required to conform to this policy; however, in the event that a specific policy requirement cannot be met as explicitly stated, agencies may submit a waiver request. The waiver request must explain the reason for the request, identify compensating controls/actions that meet the intent of the policy, and identify how the compensating controls/actions provide a similar or greater level of defense or compliance than the policy requirement. Agencies and staff offices shall address all policy waiver request memorandums to the USDA CISO and submit the request to asoc.outreach@asoc.usda.gov for review and decision.

b. Unless otherwise specified, agencies must review and renew approved policy waivers every fiscal year. Approved waivers must be associated with a NIST security control and tracked as a plan of action and milestones item in the Department's FISMA data management and reporting tool. The USDA CISO shall monitor and approve waivers to this policy.

-END-

APPENDIX A

DEFINITIONS

a. Awareness. A learning process that sets the stage for training by changing individual and organizational attitudes to realize the importance of security and the adverse consequences of its failure. Source: NIST SP 800-16, April, 1998.

b. Information System. A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. Source: OMB Circular A-130, Appendix III

c. Risk. The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals; resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring. Source: NIST SP 800-30, Rev 1, September 2012.

d. Training. A learning experience in which an individual is taught to execute a specific information security procedure or understand the information security common body of knowledge. Training strives to produce relevant and needed security skills and competencies.

APPENDIX B

ACRONYMS AND ABBREVIATIONS

AAR	Acquisition Approval Request
ACIO	Associate Chief Information Officer
ASOC	Agriculture Security Operations Center
CIO	Chief Information Officer
CISO	Chief Information Security Officer
DHS	Department of Homeland Security
DM	Departmental Manual
DR	Departmental Regulation
FISMA	Federal Information Security Management Act
ISSLOB	Information Systems Security Line of Business
ISSPM	Information Systems Security Program Manager
IT	Information Technology
NIST	National Institute of Standards and Technology
OMB	Office of Management and Budget
SP	Special Publication
USDA	United States Department of Agriculture

APPENDIX C

REFERENCES AND AUTHORITIES

Department of Homeland Security (DHS) Information Systems Security Line of Business

DM 3510-001, *Physical Security Standards for Information Technology (IT) Restricted Space*, August 19, 2004

DR 3300-001, *Telecommunications & Internet Services and Use*, March 23, 1999

DR 3620-001, *USDA eLearning Services, Courseware and Content*, October 29, 2004

DR 3630-001, *USDA Enterprise Shared Services (ESS)*, June 1, 2005

DR4070-735-001, *Employee Responsibilities and Conduct*, October 4, 2007

Federal Information Security Management Act of 2002 (FISMA), 44 U.S.C. 3531 et seq.(2013)

NIST Information Technology Laboratory (ITL) Bulletin, *How to Identify Personnel with Significant Responsibilities for Information Security*, June 2010

NIST SP 800-137, *Information Security Continuous Monitoring for Federal Information Systems and Organizations*, September 2011

NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model*, April, 1998

NIST SP 800-18, Revision 1, *Guide for Developing Security Plans for Federal Information Systems*, February 2006.

NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, February 2010

NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program*, October 2003

NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*, August 2009

NIST SP 800-60, Volume 1, Revision 1, *Guide for Mapping Types of Information and Information Systems to Security Categories*, August 2008

OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, as amended